REMARKS

This paper is being provided in response to the December 23, 2004 Final Office Action for the above-referenced application. In this response, Applicants have canceled Claims 9-12, 17, 21, 23-25, 31-35, 37, 38 and 48, and amended Claims 1, 22, 26, 36, 39, and 47 in order to clarify that which Applicants deem to be the invention. Applicants respectfully submit that the amendments to the claims are all supported by the originally-filed application.

The rejection of Claims 1-16, 18-42, and 44-50 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,338,141 to Wells, (hereinafter "Wells") in view of Frisch Essential System Administration (hereinafter, "Frisch") and Kim "The Design and Implementation of Tripwire: A File System Integrity Checker" (hereinafter "Kim") is hereby traversed and reconsideration thereof is respectively requested in view of amendments to claims contained herein. Applicant notes that this rejection as applied to Claims 9-12, 21, 23-25, 31-35, 37, 38, and 48 is moot in view of the cancellation of these claims herein.

Claim 1, as amended herein, recites a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; an antivirus unit, that uses a particular operating system, scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned by the antivirus unit includes at least some parts of the first and second segments; and the antivirus unit accessing non-native files created using operating systems different from the particular

operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses, wherein said antivirus unit accesses one of the segments without using file-based information of any host having access to said segment. Claims 2-8, 13-16 and 18-20 depend from Claim 1.

Claim 22, as amended herein, recites a method of scanning a storage device for viruses, comprising: performing a first virus scan at a first time; and performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing a part of the storage device that is also accessible to at least one host, said accessing of said part is performed without using file-based information of any host having access to said segment.

Claim 26, as amended herein, recites a computer program product for detecting computer viruses, comprising: means for accessing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; means that uses a particular operating system for scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned includes at least some parts of the first and second segments; and means for

accessing non-native files created using operating systems different from the particular

operating system that is used in connection with scanning at least parts of the disk space for

viruses, wherein, when performing a virus scan accessing one of the segments that is also

accessible to at least one of said plurality of hosts, said accessing of said segment is

performed without using file-based information of any host having access to said segment.

Claims 27-30 depend, directly or indirectly, from Claim 26.

Claim 36, as amended herein, recites a computer program product for scanning a

storage device for viruses, comprising: means for performing a first virus scan at a first time;

and means for performing a second virus scan at a second time after the first time, wherein

for said second virus scan, logical entities having a date of last modification that is after the

first time are examined and wherein performing said first and second virus scans includes

using a particular operating system and accessing non-native files created using operating

systems different from the particular operating system, wherein, when performing a virus

scan accessing a part of the storage device that is also accessible to at least one host, said

accessing of said part is performed without using file-based information of any host having

access to said segment.

Claim 39, as amended herein, recites an antivirus scanning unit, comprising:

means for coupling to at least one storage device having at least a portion that is partitioned

into separate segments, each segment being accessed by at least one of a plurality of hosts,

wherein a first one of the segments is accessed using a different file system than a second one

of the segments; means for using a particular operating system for scanning at least part of

the at least one storage device for viruses, wherein the part that is scanned includes at least some parts of the first and second segments; and means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses, wherein, when performing a virus scan accessing one of the segments that is also accessible to at least one of said plurality of hosts, said accessing of the segment is performed without using file-based information of any host having access to said segment. Claims 40-42 and 44-46 depend from Claim 39.

Claim 47, as amended herein, recites an antivirus unit, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing a part of the storage device that is also accessible to at least one host, said accessing of said part is performed without using file-based information of any host having access to said segment. Claims 49-50 depend from Claim 47.

Wells relates to a stand-alone computer process that uses a single information engine to produce a collection of relational data to detect computer viruses in computer files. The entire process is performed on a single, stand-alone computer system in real time. The

process can also be run on the stand-alone system from a connected, remote computer system, which remote system can maintain the known virus databases. (See Abstract; Col. 1, Lines 5-20). Wells discloses a system called Raven as part of a virus detection tool. Raven is run on a given system and the gathered data for each file checked is tested against the relational data that represents the known viruses stored in a virus-detection database. An exact match of all related data indicates a known virus is present. In addition, if most, but not all, of the data is matched, there is a high probability that an unknown (but closely related) virus is present. (Col. 2, Lines 54-62; Figure 5). Page 3 of the Office Action states that Wells does not expressly disclose providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments.

As set forth on pages 3 and 4 of the Office Action, Frisch teaches a UNIX operating system that enables a flexible partitioning capability wherein each partitioned segment is accessed using a different file system. Page 587 of Frisch also discloses that TCP/IP provides a number of user commands to access remote systems. The commands include ftp which allows users to copy files between a local system and any reachable system.

As set forth on page 4 of the Office Action, Kim teaches selectively checking the integrity of separate file systems on a disk using the UNIX tool tripwire.

Applicants respectfully submit that the references, taken separately or in combination, neither disclose nor suggest Claim 1, as amended herein, in that the references neither disclose nor suggest *a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ... wherein said antivirus unit accesses one of the segments without using file-based information of any host having access to said segment,* as set forth in amended Claim 1. Wells discloses gathering data about files which is tested against relational data to detect the presence of a virus. Processing as described, for example, in Wells' Figure 5, step 2, simply accesses a file for processing by Raven. Wells appears silent regarding any mention of another entity, such as a host, having access to a file processed in connection with virus detection. Thus, Wells cannot possibly disclose or suggest anything regarding file-based information of any such host.

Frisch discloses dividing a disk into partitions each holding its own file system, but appears silent regarding any mention of what information is used in connection with accessing a segment by an antivirus unit. Kim also appears to disclose generally operating on files, but appears to make no disclosure or suggestion of a portion of a device being accessed for virus detection that is also accessible to a host. Further, Kim appears silent regarding any mention of what information may or may not be used in connection with virus detection.

Accordingly, the references neither teach, disclose or suggest at least the features of *a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least*

one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ... wherein said antivirus unit accesses one of the segments without using file-based information of any host having access to said segment, as set forth in amended Claim 1.

For reasons similar to those set forth regarding Claim 1, Applicant's amended Claim 22 is also neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest *a method of scanning a storage device for viruses, comprising: ... wherein, when performing a virus scan accessing a part of the storage device that is also accessible to at least one host, said accessing of said part is performed without using file-based information of any host having access to said segment,* as set forth in Claim 22.

For reasons similar to those set forth regarding Claim 1, Applicant's amended Claim 26 is also neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest *a computer program product for detecting computer viruses, comprising: means for accessing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ... wherein, when performing a virus scan accessing one of the segments that is also accessible to at least one of said plurality of hosts, said accessing of said segment is performed without using file-based information of any host having access to said segment,* as set forth in Claim 26.

For reasons similar to those set forth regarding Claim 1, Applicant's amended Claim 36 is also neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest *a computer program product for scanning a storage device for viruses, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, ..., wherein, when performing a virus scan accessing a part of the storage device that is also accessible to at least one host, said accessing of said part is performed without using file-based information of any host having access to said segment,* as set forth in Claim 36.

For reasons similar to those set forth regarding Claim 1, Applicant's amended Claim 39 is also neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest *an antivirus scanning unit, comprising: means for coupling to at least one storage device having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ..., wherein, when performing a virus scan accessing one of the segments that is also accessible to at least one of said plurality of hosts, said accessing of the segment is performed without using file-based information of any host having access to said segment,* as set forth in Claim 39.

For reasons similar to those set forth regarding Claim 1, Applicant's amended Claim 47 is also neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest *an antivirus unit, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, ..., wherein, when performing a virus scan accessing a part of the storage device that is also accessible to at least one host, said accessing of said part is performed without using file-based information of any host having access to said segment,* as set forth in Claim 47.

In view of the foregoing, Applicants respectfully request that this rejection be reconsidered and withdrawn.

The rejection of Claim 17 under 35 U.S.C. § 103(a) as being unpatentable over Wells in view of Frisch and Kim and further in view of Stang "Comparison: Products to Detect Changes to Programs" (hereinafter "Stang") is rendered moot in view of the cancellation of Claim 17 herein.

The rejection of Claim 43 under 35 U.S.C. § 103(a) as being unpatentable over Wells in view of Frisch and Kim and further in view of U.S. Patent No. 6,088,803 to Tso, et al. (hereinafter "Tso") is hereby traversed and reconsideration thereof is respectively requested in view of amendments to claims contained herein.

Claim 43 depends from independent Claim 39. For reasons set forth above, Wells, Frisch and Kim neither disclose nor suggest Claim 39. For reasons set forth below, combining Wells, Frisch and Kim with Tso also neither discloses nor suggests Claim 39, and claims that depend therefrom.

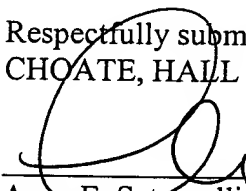Wells, Frisch, and Kim are also discussed above.

As set forth on pages 16-17 of the Office Action, Tso discloses an antivirus accelerator for computer networks wherein an antivirus unit is interposed between a storage device and a host.

Applicants respectfully submit that combining Tso with the references of Wells, Frisch and Kim does not overcome the deficiencies of Wells, Frisch, and Kim with respect to Applicant's amended Claim 39, as discussed above, from which Claim 43 ultimately depends.

In view of the foregoing, Applicants respectfully request that this rejection be reconsidered and withdrawn.

Based on the above, Applicants respectfully request that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 617-248-4042.

Respectfully submitted,
CHOATE, HALL & STEWART LLP

Anne E. Saturnelli
Reg. No. 41,290

Choate, Hall & Stewart LLP
Patent Group
Exchange Place
53 State Street
Boston, MA 02109-2804
Tel.: (617) 248-5000
Fax: (617) 248-4000

Date: March 1, 2005